INVERTIBILITY OF MODULES OVER PRÜFER RINGS

BY

HOWARD GORMAN[1]

0. Introduction.

The study of orders has grown out of an attempt to generalize the results of algebraic number theory to non commutative algebras. In this study, the ground ring has remained a Dedekind ring and the full ring of integers has been replaced by maximal orders in a finite-dimensional algebra L with 1 over K, the quotient field of R.

One of the main results of this theory is that certain ideals of maximal orders are invertible [1] (in fact, locally principal [2], [7]) in an appropriate sense. These modules are distinguished by the fact that they are finitely generated as R-modules and span L over K. On the other hand, it is standard that with with any module of the above type contained in L, we can associate two orders (not necessarily maximal) and give a definition of invertibility. This suggests that we deal with invertibility from a different point of view. We shall consider the modules as the basic units of study and pose questions of invertibility about them. In this way, all orders are brought into play, not just the maximal ones. This point of view is further motivated by Dedekind's description of the composition of quadratic forms with rational coefficients in terms of multiplication of modules [3] (recently generalized by Kaplansky to Bezout domains [4]) and by a result of Dade, Taussky and Zassenhaus [5], which says that when L is a field such that $(L:K) = n$, the $(n - 1)$-st power of any module is invertible.

If the study of modules is restricted to the distinguished ones with invertibility the goal, it is natural to ask of the ground ring only that it fulfil this goal with respect to its quotient field. So, theorems proving invertibility will require only that R be a Prüfer ring (a commutative domain with 1 with every non-zero, finitely generated ideal invertible).

The general notation of this paper is as follows. R will always be a commutative domain with 1 and will have quotient field K. L will always be a finite-dimensional algebra with 1 over K. We shall use $\oplus$ to mean a module direct sum and $\dotplus$ to mean a ring direct sum.

In I, we give the basic definitions and prove some preliminary results. In II, we show that the Dade, Taussky Zassenhaus result generalizes to the case where R is a Prüfer ring and L is a commutative algebra. Using this result, we show that if T is the integral closure of R in L, then any ideal of T which

Received April 12, 1968.

[1] These results are contained in the author's Ph.D. thesis done at the University of Chicago in 1968 under the direction of I. Kaplansky. It is a pleasure to thank Dr. Kaplansky for his help and encouragement.

contains a non zero divisor of L is invertible in T. This says, in particular, that when L is a field, T is a Prüfer ring. We also prove a new result concerning the local principality of invertible modules. In III, we give two conditions on L, each of which is enough to insure that L contain a non invertible module. We show, also, that if L satisfies neither condition, and if R is a Prüfer ring, then L contains only invertible modules.

I. Preliminaries.

1. Basic concepts. We now make explicit the concepts mentioned in the introduction.

DEFINITION. An R-module contained in L is called *admissible* if it is finitely generated over R and generates L over K. We shall be concerned with admissible modules only so that, from now on, unless otherwise stated, all modules will be assumed admissible.

DEFINITION. A subring P of L is called an *order* if it is admissible as an R-module and contains R. We note that, since P is finitely generated over R, all its elements are integral over R.

DEFINITION. Let A be any R-module contained in L. We call

$$P = \{x \in L \mid xA \subset A\}$$

the *left order* of A,

$$Q = \{x \in K \mid Ax \subset A\}$$

the *right order* of A and

$$A^{-1} = \{x \in L \mid AxA \subset A\}$$

the *inverse* of A. We write $A = {}_PA_Q$ to indicate that P and Q are the left and right orders of A respectively. We say that A is *left* (resp. *right*) *invertible* if $A^{-1}A = Q$ (resp. $AA^{-1} = P$) and that A is *invertible* if it is both left and right invertible. It is clear that both P and Q contain R. When A is admissible, P and Q will consist of integral elements and it is easy to see that P, Q and A^{-1} all generate L over K. We shall show shortly that, when R is a Prüfer ring, P, Q and A^{-1} are finitely generated as well. Hence, when R is a Prüfer ring, P and Q are orders and A^{-1} is admissible.

Note that if $A = {}_PA_Q$,then A^{-1} is a left Q-module and a right$P$-module, although P and Q are not necessarily its orders. If L is commutative, the left and right orders of A are equal and we write P_A for the order of A. We remark, finally, that R will be assumed infinite throughout, since otherwise $R = K$ and questions of invertibility become trivial.

2. A norm and localization. For any $x \in L$, we define $N(x)$, the *norm* of x, to be the determinant of x in the right regular representation of L. Thus, taking norms defines a multiplicative map from L to K. Using the norm, we define a map from modules to fractional ideals of R as follows. For any module A, we let $N(A)$ be the fractional ideal of R generated by the norms of the elements of A. We call $N(A)$ the norm of A. We remark that this latter map is not, in general, multiplicative nor is $N(A)$, in general, finitely generated. An example of these facts will appear later.

Localization is a valuable tool in dealing with both the question of invertibility and with the question of when the norm is multiplicative on modules. For, standard arguments show that a module A is invertible if and only if A_M is invertible (as an R_M-module) and that, given modules A and B, $N(AB) = N(A)N(B)$ if and only if $N(A_M B_M) = N(A_M)N(B_M)$ where M runs over the maximal ideals of R. The value of localization as a tool derives from the well known fact that the ring R is a Prüfer ring if and only if R_M is a valuation ring for each maximal ideal M of R.

3. Admissibility of orders and inverses.

We show that, when R is a Prüfer ring, orders and inverses of admissible modules are admissible.

LEMMA 1. *Let A be an admissible module. Then A is generated by invertible elements of L.*

Proof. Let $A = (t, x_1, \cdots, x_n)/R$ with $t \in K$ and $t \neq 0$. Then, for any $r \in R$, $x_i - tr \in A$. Since L is finite dimensional over K, $x_i - tr$ is invertible if and only if it is a non-zero divisor as an element of $\mathrm{End}_K L$, i.e., if and only if $N(x_i - tr) \neq 0$, i.e., if and only if tr is not a characteristic root of x_i. Since R is an infinite domain, we may choose $r_0 \in R$ so that tr_0 is not a characteristic root of any x_i. Since

$$A = (t, x_1 - tr_0, \cdots, x_n - tr_0)/R,$$

we are done.

It is a well known fact [6] that if M is any R-module with submodules I_1 and I_2 such that I_1, I_2 and $I_1 + I_2$ are finitely presented, then $I_1 \cap I_2$ is finitely generated. When we apply this fact to our setup, we get the following. If A_1 and A_2 are any finitely generated R-modules contained in L, then A_1, A_2 and $A_1 + A_2$ are torsion free and so, since R is a Prüfer ring, they are projective and, a fortiori, finitely presented. Hence $A_1 \cap A_2$ is finitely generated. If A_3 is another finitely generated R-module contained in L, then applying the above argument to $A_1 \cap A_2$ and A_3, we see that $A_1 \cap A_2 \cap A_3$ is finitely generated. Continuing in this way, we see that the intersection of a finite number of finitely generated R-modules contained in L is finitely generated. This enables us to prove the following

LEMMA 2. *Let R be a Prüfer ring. Let A and B be finitely generated R-modules contained in L such that A is generated by units of L.* Let

$$C = \{x \in L \mid xA \subset B\}. \text{ Then } C \text{ is finitely generated.}$$

Proof. Let $A = (x_1, \cdots x_n)/R$ with each x_i a unit of L. Then

$y \in C \Leftrightarrow yA \in B \Leftrightarrow yx_i \in B$ for each $i \Leftrightarrow y \in Bx_i^{-1}$ for each i. Hence, $C = \bigcap_{i=1}^{n} Bx_i^{-1}$. Since R is a Prüfer ring, the remarks preceding the lemma may be used to complete the argument.

As a corollary, we deduce the desired result.

COROLLARY. *Let R be a Prüfer ring and let $A = {}_PA_Q$ be an admissible module. Then P, Q and A^{-1} are admissible.*

Proof. We need only prove finite generation. For P and Q, this follows immediately from Lemma 2 and the definitions. As for A^{-1}, it is enough to note that it could be equally well defined as the set of all $x \in L$ such that $xA \subset Q$.

We remark, finally, that if R is a valuation ring and if $(L:K) = n$, then any admissible module is free on n generators. For, any free basis would have to have exactly n elements and a free basis always exists since finitely generated projectives over quasi-local rings are free.

II. Invertibility of powers of modules.

1. Dade, Taussky and Zassenhaus [5] have shown that when R is a Dedekind ring and L is an n-dimensional field extension of K, then A^{n-1} is invertible for any admissible module A. We generalize this result to the following.

THEOREM 1. *Let R be a Prüfer ring with quotient field K. Let L be a commutative, n-dimensional algebra with* 1 *over K. Let A be an admissible module. Then A^{n-1} is invertible.*

We prove the theorem by a series of lemmas and assume, unless otherwise stated, that L is commutative and that R is a valuation ring.

It is a standard result that if F is any infinite field and if $f(x_1, \cdots, x_n)$ is a polynomial over F which is not the zero polynomial, then f is not identically zero on F. We use this fact to prove

LEMMA 3. *Let R be a valuation ring with maximal ideal M such that R/M is infinite. Let $f(x_1, \cdots x_n)$ be a polynomial with domain R and coefficients in K. Then the fractional R-ideal generated by the image of f is generated by the coefficients of f.*

Proof. Since R is a valuation ring, f has a minimal coefficient; call it k. Then

$$f(x_1, \cdots, x_n) = kg(x_1, \cdots, x_n)$$

where g has a coefficient equal to 1 and all coefficients in R. Hence, the coefficients of g generate R. Now the image of g is contained in R and $g(\text{mod } M) \not\equiv 0$, so that g has a value which is a unit of R. So the fractional R-ideal generated by the image of g is R. Therefore, the lemma is true for g and so for f.

DEFINITION. Let A be any R-module contained in L. We say that $x \in A$ has *minimal norm* in A if, for every $y \in A$, $N(x)$ divides $N(y)$.

Assume that R satisfies the conditions of Lemma 3, and that A is an R-module. Then the norm form on A with respect to some fixed basis of A over R is a polynomial satisfying the conditions of Lemma 3 so that the ideal generated by its image, i.e. $N(A)$, is finitely generated. Since $N(A)$ is generated by the norms of its elements, a finite number of these norms suffice. By choosing an element of A corresponding to the minimal of these norms, we prove

LEMMA 4. *Let R be a valuation ring with maximal ideal M such that R/M is infinite. Let A be an admissible module. Then A contains an element of minimal norm (i.e. $N(A)$ is principal).*

We remark that when A is admissible and $x \in A$ is an element of minimal norm, then x is invertible. For, since A is admissible, it contains some non zero element t of K. Since $N(t) = t^{\dim L} \neq 0$, $N(A) \neq 0$ and so $N(x) \neq 0$. Hence x is invertible as noted in Lemma 1.

The importance of an element of minimal norm is revealed in:

LEMMA 5. *Let R be a valuation ring with maximal ideal M such that R/M is infinite. Let A be an admissible module with $x \in A$ having minimal norm. Then $B = x^{-1}A$ consists entirely of elements integral over R.*

Proof. Choose any $z \in B$. Since $1 \in B$, we have that $z - u \in B$ for any $u \in R$, and so $N(z - u) \in R$. Now $N(z - u) = u^n + a_{n-1}u^{n-1} + \cdots + a_0$, the characteristic polynomial for z. Choose $u_1, \cdots, u_{n-1}$ units of R with u_i and u_j in different cosets of R/M for $i \neq j$. Substituting these units for u and noting that $a_0 = N(z)$, we get the system of equations

$$a_{n-1}u_i^{n-2} + \cdots + a_1 = r_i \in R, \qquad i = 1, \cdots, n-1.$$

Now the system of equations

$$X_{n-1}u_i^{n-2} + \cdots + X_1 = r_i \in R, \qquad i = 1, \cdots, n-1,$$

has a unique solution in R if its determinant is a unit of R. But the determinant is the Vandermonde determinant and equals $\prod_{i<j}(u_i - u_j)$ which is a unit of R. Since $a_1, \cdots, a_{n-1}$ is manifestly a solution, each $a_i \in R$. Since z satisfies its characteristic polynomial, it is integral over R and we are done.

This lemma motivates the following

DEFINITION. An admissible module which contains 1 and consists of integral elements (over R) is called a *semi-order*.

In the language of this definition, we have shown in Lemma 5, that $B = x^{-1}A$ is a semi-order. We give some simple properties of semi-orders.

LEMMA 6. *If B is a semi-order, then some power of B is an order.*

Proof. Since B is finitely generated with each generator satisfying a monic polynomial with integral coefficients and since L is commutative, it is easy to see that there is a positive integer m such that $B^m \subset B^{m-1}$. Hence, B^{m-1} is an order.

LEMMA 7. *Suppose that L (not necessarily commutative) has radical T. Suppose that A is a semi-order such that $A' = A \pmod{T}$ is an order. Then some power of A is an order.*

Proof. Since $(A')^2 = A'$, we know that $A^2 \subset A + T$. Now, there is an integer t such that $T^t = 0$. Choose $x_1, \cdots, x_t \in A^2$. Then there are $y_i \in A$ and $n_i \in T$ such that $x_i = y_i + n_i$. Then

$$\textstyle\prod_{i=1}^t (x_i - y_i) = \prod_{i=1}^t n_i = 0.$$

Expanding the left hand side, we see that $\prod_{i=1}^t x_i$ is contained in A^{2t-1}. Since $\prod_{i=1}^t x_i$ has the form of an arbitrary generator of A^{2t}, we have $A^{2t} \subset A^{2t-1}$, i.e., A^{2t-1} is an order.

We note that if L/T is commutative, the preceding two lemmas imply that some power of any semi-order is an order.

We can now show that when R/M is infinite, some power of any module is invertible. For if $B = x^{-1}A$ (in the notation of Lemma 5), then B is a semi-order and by Lemma 6 there is an integer m such that $B^m = x^{-m}A^m$ is an order. Then $A^m = x^m B^m$ is invertible with inverse $x^{-m}B^m$. Therefore, to prove Theorem 1 when R/M is infinite, we need only show that we can choose $m = n - 1$. We follow the technique in [5].

LEMMA 8. *Let S be an n-dimensional, commutative algebra with 1 over a field F. Let V be a linear subspace of S, containing 1 and such that V generates S as an algebra over F. Then $V^{n-1} = S$.*

Proof. The conditions on V imply that $(V:K) > 1$ and that $\dim_K V^i \geq \dim_K V^{i-1} + 1$ as long as V^{i-1} is contained in S properly. It follows that $V^{n-1} = S$.

Now B^m is free on n generators; hence, $(B^m/MB^m : R/M) = n$. Set

$$V = (B + MB^m)/MB^m.$$

Then, by Lemma 8, $V^{n-1} = B^m/MB^m$. Therefore, $B^{n-1} + MB^m = B^m$ and the result follows from Nakayama's lemma, i.e., we have proved Theorem 1 when R/M is infinite.

Suppose that R/M is finite. We employ the following well known device. Let $R_0 = R[x]_{MR[x]}$, i.e., R_0 is the ring whose elements are the rational functions $f(x)/g(x)$ where x is an indeterminate, $f, g \in R[x]$, and g has some coefficient a unit of R. Then R_0 is a valuation ring and its quotient field is just

$K(x)$. Let $L_0 = LK(x)$ and $A_0 = AR_0$ for any admissible module A. Then A_0 is an admissible R_0-module. Since R_0/MR_0 is infinite and $(L_0:K(x)) = n$, we have that A_0^{n-1} is invertible. The following two lemmas show that A^{n-1} is invertible.

LEMMA 9. *Let B be an admissible R-module and let $B_0 = BR_0$. Then $p(x)/q(x) \in (B_0)^{-1}$ if and only if the coefficients of $p(x)$ are in B^{-1}.*

Proof. The "if" part is obvious. For the "only if" part, let p_1/q_1 and p_2/q_2 be in B_0 and $p/q \in (B_0)^{-1}$. It is sufficient to prove the result when p_1 and p_2 are in $B \subset B_0$. Then $p_1\, pp_2$ has coefficients in B. The result is clear once we have written out p as a polynomial and carried out the multiplication.

LEMMA 10. *Let B be an admissible R-module. Then, if BR_0 is invertible, so is B.*

Proof. Let $1 = \sum_{i=1}^{r} (p_i/q_i)(p_i'/q_i')$ with $p_i/q_i \in B_0$ and $p_i'/q_i' \in B_0^{-1}$. Since some coefficient of $\prod_{i=1}^{r} q_i\, q_i'$ is a unit u, say, of R, we get from

$$\prod_{i=1}^{r} q_i\, q_i' = \sum_{i=1}^{r} p_i\, p_i' \left(\prod_{j\neq i} q_j\, q_j'\right)$$

that $u = \sum_{i=1}^{s} a_i\, b_i$ where $a_i \in B$ and $b_i \in B^{-1}$ by Lemma 9. Therefore, $1 \in BB^{-1}$ and we are done.

We have shown that A^{n-1} is invertible for any admissible module A and so, have completed the proof of Theorem 1.

It is well known that, when R is a Prüfer ring and L is a finite-dimensional field extension of K, then the integral closure of R in L is again a Prüfer ring. Theorem 1 provides the following generalization.

LEMMA 11. *Let R be a Prüfer ring with quotient field K. Let L be a finite-dimensional, commutative algebra with 1 over K. Let S be the integral closure of R in L. Let A be a finitely generated S-module contained in L which contains a non-zero divisor of L. Then A is invertible.*

Proof. Since S contains a basis of L over K and A contains a non-zero divisor (i.e. a unit), we know that A contains a basis of L over K. Let $a_1, \cdots, a_n$ be a generating set for A over S which contains a basis of L over K. Let $A_0 = (a_1, \cdots, a_n)/R$. Then A_0 is admissible. Since A_0^m is invertible with inverse B, say, for some integer m and since all orders are contained in S, we have that $S = A_0^m BS = A(A^{m-1}B)$, since $A_0 S = A$. Hence, A is invertible by Lemma 15.

2. An extension to the non commutative case. We may ask to what extent the result of Theorem 1 is true when L is no longer assumed to be commutative. Assume that R is a valuation ring with infinite residue class field. If we examine the relevant proofs in the preceding section, we see that the existence of an element of minimal norm and the fact that $B = x^{-1}A$ is a semi-order are independent of the commutativity of L. Suppose that L has the property that some power of any semi-order is an order. Then there is an integer m such that $(x^{-1}A)^m = CA$ is an order where C is the admissible module $(x^{-1}A)^{m-1}x^{-1}$. Since L has the above property when it is commutative modulo its radical, the above discussion is meaningful and proves the following

LEMMA 12. *Let R be a valuation ring with maximal ideal M such that R/M is infinite. Let L have the property that some power of any semi-order is an order. Let A be an admissible module. Then there are admissible modules C and D such that CA and AD are orders.*

3. Principal modules. Dade, Taussky and Zassenhaus [5] show, also, that when R is a quasi-local domain and A is a fractional ideal of R, then A is invertible if and only if it is principal. We generalize this result in Lemma 13, but first we remind the reader of some well known facts and motivate the lemma.

DEFINITION. Let $A = {}_PA_Q$ be any R-module contained in L. We say that A is left (right) principal if there is an $x \in L$ such that $A = Px$ $(=xQ)$.

If A is admissible, it is clear that x is a unit of L so that Px is invertible with inverse $x^{-1}P$. Further, $A = x(x^{-1}Px)$ and it is easy to check that $x^{-1}Px = Q$, so that left principal implies right principal.

If R is any quasi-local ring (a commutative ring with 1, with a unique maximal ideal) with maximal ideal M and S is an R-algebra with 1, finitely generated as an R-module. Then it is well known that $MS \subset J(S)$, the Jacobson radical of S. Since S/MS is a finite dimensional vector space over R/M, it is Artinian; then $S/J(S)$ is Artinian over R/M and it follows that S has only a finite number of maximal, 2-sided ideals. In the context of this paper, this implies that orders over quasi-local rings have only a finite number of maximal 2-sided ideals.

Since $MS \subset J(S)$, MS is contained in every maximal left ideal of S and so there is a one to one correspondence between the maximal left ideals of S and those of S/MS by the obvious map. Hence $J(S/MS) = J(S)/MS$ and, since S/MS is Artinian over R/M, we have that $J(S)/MS$ is the radical of S/MS.

Now, let $M_1, \cdots, M_n$ be all the maximal 2-sided ideals of S and suppose that S/M_i is a division ring for each i. Then each M_i is a maximal left ideal and, so, $MS \subset \bigcap_{i=1}^n M_i$. But the maximal 2-sided ideals of S/MS are just the M_i/MS, and it follows from Wedderburn's theorem that the radical of S/MS is $\bigcap_{i=1}^n (M_i/MS) = (\bigcap_{i=1}^n M_i)/MS$. It follows that $J(S) = \bigcap_{i=1}^n M_i$.

For a concrete example of the above situation, we might choose R quasi-local and L with radical T such that L/T is commutative (triangular $m \times m$ matrices over K will do). Then an order P with maximal ideals $M_1, \cdots, M_n$ takes on the role of the algebra S in the above discussion. Since T is nilpotent, so is $T \cap P$, and it follows that $T \cap P$ is contained in each M_i. Since $p_1p_2 - p_2p_1 \in T$

for any $p_1, p_2 \in P$, we have that $P/T \cap P$ is commutative. Therefore

$$P/(\bigcap_{i=1}^n M_i) = \prod_{i=1}^n P/M_i,$$

with each P/M_i a field.

LEMMA 13. *Let R be a domain with quotient field K. Let $A = {}_PA_Q$ be admissible. Let $M_1, \cdots, M_n$ be all the maximal 2-sided ideals of P and assume that P/M_i is a division ring for each i. Assume, further, that $J(P) = \bigcap_{i=1}^n M_i$. Then A is invertible if and only if it is principal.*

Proof. The "if" part of the lemma follows from preceding remarks. For the "only if" part, it is enough to show that $AA^{-1} = P$ implies that A is left principal. Suppose that $AA^{-1} = P$. Then there are $a_i \in A$ and $b_i \in A^{-1}$ such that $a_i b_i \notin M_i$ for each i. Since

$$(1) \qquad P/(\bigcap_{i=1}^n M_i) = \prod_{i=1}^n P/M_i,$$

there are $e_i \in P$ such that $e_i \equiv 1 \pmod{M_i}$ and $e_i \equiv 0 \pmod{M_j}$ for $i \neq j$. Let $a = \sum_{i=1}^n e_i a_i$ and $b = \sum_{i=1}^n b_i e_i$. Then $ab \in P$ and $ab \equiv a_i b_i \not\equiv 0 \pmod{M_i}$ for each i. Suppose that this implies that ab is left invertible in P. Then, since $Ab \subset P$ and is a left P-ideal containing the left unit ab, we have that $Ab = P$. But b is a unit of L (it is a non-zero divisorin $\mathrm{End}_K L$). So $A = Pb^{-1}$ and we have proved the result.

It remains to prove that ab is a left unit of P. Since ab is not contained in any M_i, it is enough to prove that any maximal left ideal of P is one of the M_i. Let I be a maximal left ideal of P distinct from the M_i. It follows that for each i

$$(2) \qquad M_1 M_2 \cdots M_{i-1} M_{i+1} \cdots M_n I \not\subset M_i.$$

Since P/M_i is a division ring for each i, (1) and (2) together imply that there are $x_i \in I$ such that $x_i \equiv 0 \pmod{M_j}$ for $i \neq j$ and $x_i \equiv 1 \pmod{M_i}$. Let $x = \sum_{i=1}^n x_i$. Then $x \equiv 1 \pmod{(\bigcap_{i=1}^n M_i)}$ so $x \equiv 1 \pmod{J(P)}$. Hence, x is a unit of P, i.e., $I = P$ and we are done.

4. The multiplicativeness and finite generation of the norm. We give the promised examples to show that the norm is not necessarily multiplicative on modules and that the norm of a module need not be finitely generated.

The first example deals with multiplicativeness. Let R be a valuation ring with maximal ideal M such that $R/M = Z_2$. (For example, R could be the ring of formal power series over Z_2.) Let $L = K \dotplus K \dotplus K$ and let A have generators $(1, 0, 1)$, $(0, 1, 1)$ and $(0, 0, t)$ over R with t a non unit of R. Then, the norm form on A is $xy(x + y + zt)$ with x, y and z arbitrary elements of R. Since $R/M = Z_2$, we need only evaluate the norm form over Z_2 to convince ourselves that $N(A) \subset M$. On the other hand, A^2 is generated by $(1, 0, 1)$, $(0, 1, 1)$ and $(0, 0, 1)$, so that $N(A^2) = R$. So, the norm is not multiplicative even on powers of modules.

We turn, now, to the finite generation of the norm. Let K be the field of infinite series whose general term x has the form $x = \sum_{n=1}^{\infty} a_n t^{b_n}$ where $a_n \in Z_2$, t is an indeterminate and the b_n's are real numbers for each positive integer n with the property that all but a finite number of them are positive and that $b_n < b_{n+1}$ for each n.

We define a valuation, v, on K by $v(x) = b_m$, where m is the smallest integer with $a_m \neq 0$. Then, the value group of v is the additive group of the real numbers. The valuation ring R associated with v is the subring of elements y of K such $v(y) \geq 0$, and the maximal ideal M of R is the subring of R consisting of elements of positive value. Then M is not finitely generated since it contains no element of minimal, positive norm. Further, $R/M = Z_2$.

We let $L = K \dotplus K \dotplus K$ and let A have generators $(1, 0, 1)$, $(0, 1, 1)$ and $(0, 0, t)$ as before, so that the norm form on A is $xy(x + y + zt)$ and $N(A) \subset M$. It suffices to show that $N(A) = M$. For this, it is enough to show that $N(A)$ contains elements of arbitrarily small, positive value. Now

$$v(xy(x + y + zt)) = v(x) + v(y) + v(x + y + zt).$$

Choose $y \in M$ such that $v(y)$ is arbitrarily small. Let x be a unit of R. Then $v(x + y + zt) = v(x) = 0$ and so, $v(xy(x + y + zt)) = v(y)$. Since $v(y)$ is arbitrarily small, we are done.

On the positive side, it is clear that the norm is multiplicative on principal modules and, in fact, on modules which are only locally principal. Fadeev [7] has shown that when L is separable and R is Dedekind, then ideals of maximal orders are modules of this latter kind. In Lemma 14, we give another criterion for the norm to be multiplicative. Preliminary to the lemma, we make the following remarks. Suppose that L has radical T and that L/T is commutative. Let A and B be semi-orders. We claim that AB is a semi-order. We need only show that for any $a \in A$ and $b \in B$, both ab and $a + b$ are integral. There is a monic polynomial $f(x)$ with integral coefficients such that $f(ab) \equiv 0 \pmod{T}$. Since T is nilpotent, it follows that ab is integral over R. The same argument applies to $a + b$, and so we have proved our claim. We note that if $x \in L$ and $n \in T$, then $N(x) = N(x + n)$. We can now prove

LEMMA 14. *Let R be a valuation ring with maximal ideal M such that R/M is infinite. Let L have radical T and suppose that L/T is commutative. Then, for any admissible modules A and B, $N(AB) = N(A)N(B)$.*

Proof. Let x and y be elements of minimal norm in A and B respectively. Then $x^{-1}A$, $y^{-1}B$ and $x^{-1}Ay^{-1}B$ are semi-orders and, so, have norm R. Since L/T is commutative, the above remark implies that $x^{-1}Ay^{-1}B$ and $x^{-1}y^{-1}AB$ have the same norm. Hence

$$N(x^{-1}A)N(y^{-1}B) = N(x^{-1}y^{-1}AB)$$

and the result follows.

Those acquainted with the literature are aware that Deuring [1] has defined a norm N_1 which, for valuation rings can be characterized as follows. If $A = (a_1, \cdots, a_n)/R$ has left order $P = (p_1, \cdots, p_n)/R$ and if $a_i = \sum_{j=1}^{n} k_{ij} p_j$, then $N_1(A) \equiv \det (k_{ij})$. The representation norm and N_1 are, in general, different. For instance, if $L = (1, u, u^2)/K$ with $u^3 = c \in R$, and $A = (1, u, tu^2)/R$ where t is a non-unit of R, it is not hard to show that $N_1(A) = t^{-1}R$ while $N(A) = R$.

III. Algebras with All modules invertible

In this section, we deal with the question of when L contains only invertible modules. We shall give two conditions, each of which is sufficient to insure that L contain a non invertible module when $R \neq K$. Then, in the spirit of this paper, we calculate all the algebras which satisfy neither condition and show that, when R is a Prüfer ring, these algebras contain only invertible modules.

1. Lemmas. Before entering the main discussion, we prove two lemmas to be used later. The first says, essentially, that when L is commutative, a module can be invertible only in its order. The second shows that, under suitable conditions, the product of invertible modules is invertible.

LEMMA 15. *Let L be commutative and let A be any R-module contained in L. Let P be an order such that $AP = A$. Let $A_1 \subset L$ be such that $AA_1 = P$. Then $P = P_A$ and A is invertible. Further, if $A_1 P = A_1$, then $A_1 = A^{-1}$.*

Proof. That $P_A \subset P$ follows from multiplying the equation $AP_A = A$ by A_1. Since the opposite inclusion is clear, $P_A = P$ and A is invertible. If $A_1 P = A_1$, then multiplying the equation $AA_1 = P_A$ by A^{-1} gives $A_1 = A^{-1}$.

DEFINITION. Let A and B be R-modules contained in L. We call the ordered pair (A, B) *concordant* if the left order of B equals the right order of A.

LEMMA 16. *Let (A, B) be a concordant pair of modules with $A = {}_PA_Q$, $B = {}_QB_{Q'}$ and $AB = {}_{P''}AB_{Q''}$. If A and B are invertible, so is AB and $(AB)^{-1} = B^{-1}A^{-1}$, $Q' = Q''$, $P = P''$.*

Proof. Multiplying the equation $ABQ'' = AB$ on the left by $B^{-1}A^{-1}$ and using concordance, we get that $Q'' \subset Q'$ and equality follows. Similarly, $P = P''$. If $x \in (AB)^{-1}$, then $xAB \subset Q'$, i.e. $xABB^{-1}A^{-1} \subset Q'B^{-1}A^{-1} = B^{-1}A^{-1}$. Since $ABB^{-1}A^{-1} = P$, we get that $x \in B^{-1}A^{-1}$ and, so, $(AB)^{-1} \subset B^{-1}A^{-1}$, i.e. $(AB)^{-1} = B^{-1}A^{-1}$. Now the invertibility of AB follows from $B^{-1}A^{-1}AB = Q'$ and $ABB^{-1}A^{-1} = P$.

COROLLARY. *Let L be commutative and let A and B be R-modules contained in L. If A and B are invertible, so is AB and $(AB)^{-1} = A^{-1}B^{-1}$. Further, $P_{AB} = P_A P_B$.*

Proof. An examination of the proof of the lemma shows that concordance is not needed when L is commutative. So, we need only prove that

$P_{AB} = P_A P_B$. This follows easily from multiplication of the equation $ABP_{AB} = AB$ by $A^{-1}B^{-1}$.

As an application of this corollary, we prove

LEMMA 17. *Let L be commutative. Then an invertible semi-order is an order.*

Proof. Let A be an invertible semi-order. We know that A^m is an order for some integer m. Since $1 \in A$, we have that $P_A \subset A$ and $A \subset A^m$. So, we need only show that $A^m \subset A$ when A is invertible. If A is invertible, then A^m is invertible in P_A by the above corollary. Since A^m is an order, $A^m = P_A$, and we are done.

2. Two conditions for non-invertibility. We give two conditions, each of which insures that L contains a non invertible module when $R \neq K$.

CONDITION A. *L is non quadratic over K, i.e., there is $u \in L$ such that* 1, *u and u^2 are linearly independent over K.*

CONDITION B. *There are x and y in L such that* 1, *x, y and xy are linearly independent over K.*

We assume that L satisfies Condition A and construct a non-invertible module. Let $u \in L$ be a non quadratic element of degree $n > 2$. It is standard that we may assume that u is integral over R. Construct the basis $1, u, \cdots, u^{n-1}, v_1, \cdots, v_m$ of L over K. Express the products $u^i v_j$, $v_j u^i$ and $v_j v_h$ as K-linear combinations of this basis for each $i = 1, \cdots, n-1$ and $h, j = 1, \cdots, m$, and let p be the product of the denominators of all the coefficients which occur. Let k be a non-unit of R. Replacing u by kpu and each v_i by $k^n p^n v_i$, we get a new basis of L over K which we fix for the rest of the discussion. Now the products $u^i v_j$, $v_j u^i$ and $v_j v_h$ are R-linear combinations of the basis elements and each coefficient in these combinations is divisible by k. Let

$$A = {}_P A_Q = (1, u, \cdots, u^{n-2}, ku^{n-1}, v_1, \cdots, v_m)/R.$$

We assert that A is not invertible. Let

$$q = r_0 + r_1 u + \cdots + r_{n-1} u^{n-1} + s_1 v_1 + \cdots + s_m v_m$$

be an arbitrary element of A^{-1}. Since $1 \in A$, $A^{-1} \subset A$, so that k divides r_{n-1}. From the fact that $1qu^i \in A$ for $0 \leq i \leq n-2$, we get that k divides $r_1, \cdots, r_{n-2}$ and from $uqu^{n-2} \in A$, we get that k divides r_0.

Suppose that $a \in A$ and $b \in A^{-1}$. When we express ab (similarly ba) as a linear combination of the basis elements, we see that the coefficient of 1 is divisible by k. Hence, if $1 \in AA^{-1}$, k would have to be a unit of R, a contradiction. So, A is neither left nor right invertible.

We deal with Condition B in a similar manner. Assume that L satisfies Condition B. Let k be a non-unit of R and let x and y in L be such that

1, x, y and xy are linearly independent over K, and integral over R. By a method similar to the one already used, we construct a basis $1, x, y, xy, v_1, \cdots, v_m$ of L over K with the property that the product of both x and y with either xy or any of the v_i, the product of xy with any of the v_i, and the products $v_i v_j$ are expressible as R-linear combinations of the basis with coefficients divisible by k. Then the module

$$A = (1, x, y, kxy, v_1, \cdots, v_m)/R$$

is not invertible. The proof proceeds in much the same way as for algebras satisfying Condition A. We let

$$q = r_0 + r_1 x + r_2 y + r_3 xy + s_1 v_1 + \cdots + s_m v_m$$

and examine the products $xq1$, $1qy$ and xqy to show that k divides each r_i. We then show that k must be a unit of R if A is to be invertible, and thus deduce the required contradiction.

3. Algebras satisfying neither condition. We shall now uncover the algebras which satisfy neither Condition A nor Condition B. If an algebra satisfies neither condition, it is clear that the same is true for its subalgebras and quotient algebras as well as for its simple components in case it is semisimple. We shall make free use of these facts in the discussion below. Assume for the remainder of the discussion that L satisfies neither condition.

Suppose that $K \subset F \subset L$ where F is a 2-dimensional field extension of K. Then, we may consider L as a vector space over F and it follows that if $L \neq F$, then $F \oplus Fy$ (and so L itself) will satisfy Condition B for any $y \in L - F$. If L does not contain such an extension, then every element of L must satisfy a quadratic equation which factors over K. Therefore, we may choose a basis $1, u_1, \cdots, u_n$ for L over K such that either $u_i^2 = u_i$ or $u_i^2 = 0$ for each i.

Suppose, in this latter case, that L is commutative and that $u_1^2 = u_1$. Then

$$(u_1 + u_i)^2 = a(u_1 + u_i) + b \quad \text{and} \quad (u_1 - u_i)^2 = c(u_1 - u_i) + d$$

for some $a, b, c, d \in K$.

Adding these equations, we get

$$2u_1^2 + 2u_i^2 = (a + c)u_1 + (a - c)u_i + (b + d).$$

Since $u_1^2 = u_1$ and $u_i^2 = 0$ or u_i, it follows that $a + c = 2$.

Subtracting the equations, we get

$$4u_1 u_i = (a - c)u_1 + 2u_i + (b - d). \tag{3}$$

Multiplying (3) by u_1, we get that

$$2u_1 u_i = (a - c + b - d)u_1$$

and comparing with (3) implies that $2 = 0$, i.e., ch $K = 2$.

If ch $K = 2$ and t is any non-zero element of K, it follows from

$$u_1^2 + (tu_i^2) = (u_1 + tu_i)^2$$

that $u_i^2 = u_i$ and that $K = Z_2$, i.e., L is a Boolean algebra over Z_2. We remind the reader that this case is of no interest for us.

We are left with the case $u_i^2 = 0$ for each i. But if x and y are elements of L such that $x^2 = y^2 = 0$, then it follows from the dependence of 1, x, y and xy that $xy = 0$. This is independent of the commutativity of L. (If x and y are dependent, xy is clearly equal to zero. If 1, x and y are independent, then, multiplying the equation $xy = e + fx + gy$ first on the left by x and then on the right by y, we get the result.) Hence, if $u_i^2 = 0$ for each i, then $L = K \oplus$ trivial algebra.

Now, assume that L is a simple algebra. Then $L = M_n(D)$, a total matrix algebra over the division ring D. If $D \neq K$, then L contains a two dimensional field extension of K and so is equal to that extension. If $D = K$, L will satisfy Condition A if $n > 2$; if $n = 2$, L is a quaternion algebra and satisfies Condition B. So, if L is simple, it equals K or a two-dimensional field extension of K.

We come, now, to the general L and we let T denote its radical. Then L/T is semi-simple. If any of its simple components is a 2-dimensional field over K, L will contain such a field and so is equal to it. If not, each simple component is just K, so that, since L/T is commutative, $L/T = K$ or $L/T = K \dotplus K$. Since $K \dotplus K$ are separable algebras over K, we know from general theory that each can be imbedded in L with T as a complementary summand, i.e., $L = K \oplus T$ or $L = (K \dotplus K) \oplus T$. Since L is quadratic and every element of T is nilpotent, we have that $x^2 = 0$ for every $x \in T$. If x and y are in T, it follows from the dependence of 1, x, y and xy that $xy = 0$ as was remarked earlier. Hence, T is a trivial algebra and so, the structure of $K \oplus T$ is clear.

We investigate further the structure of $L = (K \dotplus K) \oplus T$. Let 1 and v be a basis for $K \dotplus K$ over K with $v^2 = v$. If $T = 0$, we need go no further. If not, choose $u \in T$, $u \neq 0$. Then

$$vu = a + bv + cu. \tag{4}$$

Hence $vu^2 = 0 = au + bvu$. If $b \neq 0$, $vu = -b^{-1}au$ which is impossible in view of (4). Also, $vu = v^2u = av + cvu$, i.e. $(1 - c)vu = av$. If $c = 1$, then $a = 0$ and $vu = u$. If $c \neq 1$, then $vu = (1 - c)^{-1}av$ which implies by (4) that $a = c = 0$, i.e. $vu = 0$. Now suppose that u and w are in T such that $vu = 0$ and $vw = w$. The above argument applied to $u + w$ gives that $v(u + w) = 0$ or $v(u + w) = u + w$. It follows that one of u and w must be zero. This implies that we have $vu = 0$ for each $u \in T$ or $vu = u$ for each $u \in T$. By symmetry, $uv = 0$ for each $u \in T$ or $uv = u$ for each $u \in T$. Since $T \neq 0$, L is not commutative. Therefore, the structure of L is as follows: it has a basis $1, v, u_1, \cdots, u_n$ where $v \in K \dotplus K$ and $u_i \in T$ for each i, and a multiplication table given by $v^2 = v$, $u_i u_j = 0$ for all i and j, $u_i v = u_i$ and $vu_i = 0$ for all i.

Consider the algebra of $m \times m$ matrices of the form

$$\left(\begin{array}{c|c} aI_1 & \# \\ \hline 0 & bI_2 \end{array}\right)$$

where $a, b \in K$, each quadrant is a block and I_1 and I_2 are identity matrices. It is easy to see that such algebras have the same structure as L does and that, for m sufficiently large, L is isomorphic to a subalgebra by the map

$$1 \to \left(\begin{array}{c|c} I_1 & 0 \\ \hline 0 & I_2 \end{array}\right), \quad v \to \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & I_2 \end{array}\right), \quad u_i \to \left(\begin{array}{c|c} 0 & E^i_{jk} \\ \hline 0 & 0 \end{array}\right)$$

for each i. For this reason, we call L an algebra of generalized 2×2 triangular matrices.

We collect our results and say what is left to be done in the following theorem.

THEOREM 2. *Let R be a commutative domain with* 1 *and with quotient field K. Let L be a finite-dimensional algebra with* 1 *over K. Then the following is true.*

1. *If L satisfies either Condition* A *or Condition* B *and $R \neq K$, then L contains a non invertible module.*

2. *If L satisfies neither condition, it is either $K \oplus$ trivial algebra, $K \dotplus K$, a 2-dimensional field extension of K or an algebra of generalized 2×2 triangular matrices, and, when R is a Prüfer ring, it will contain only invertible modules.*

Proof. It remains to prove that the algebras in the second statement contain only invertible modules and, for this, we may assume that R is a valuation ring.

We equip each of these algebras with an involution * as follows.

(i) When L is a 2-dimensional field extension, * is the non-trivial Galois automorphism when it exists and the identity otherwise.

(ii) If $L = K \dotplus K$, then $(a, b)^* = (b, a)$.

(iii) If $L = K \oplus$ trivial algebra, then * is the identity on K and $u^* = -u$ for each u in the trivial algebra.

(iv) When L is an algebra of generalized 2×2 triangular matrices, we embed L in a matrix algebra in the way previously described so that $I_1 = I_2$ and use the involution defined by interchanging a and b and replacing the matrix $\#$ by $-\#$.

This involution induces a norm N_1 on L defined by $N_1(x) = xx^*$ for each $x \in L$. In each case, $N_1(x) \in K$ and $N_1(xy) = N_1(x)N_1(y)$ for any $x, y \in L$.

Let A be an admissible module. Since N_1 is defined via an involution, $N_1(A)$ is finitely generated, so that A contains an element of minimal norm with respect to N_1. Call it x and let $P = x^{-1}A$. We claim that R is a pure submodule of P. For, suppose that there are $a \in R$ and $u \in P$ such that $au \in R$. Therefore $u \in a^{-1}R$, i.e., $u \in K$. Hence $N_1(u) = u^2$ and so, $u^2 \in R$ since norms of elements in P are in R. Since R is integrally closed in K, $u \in R$. So R is pure. Since R is a pure submodule, it is a direct summand of P, so that we may include 1 in a free basis of P over R.

We complete the proof of the theorem by showing that P is a ring. For once this is known, it is easily seen that P is the right order of A so that A is principal and, so, invertible. We separate into cases.

(i) If L is 2-dimensional, it is commutative so that A is invertible directly as a corollary to Theorem 1.

(ii) Suppose that $L = K \oplus$ trivial algebra. Fix a basis $1, v_1, \cdots, v_n$ for L over K, with $v_i \in$ trivial algebra for each i. Let $1, u_1, \cdots, u_n$ be a basis for P over R. Then $u_i = a_i + \sum_{j=1}^{n} a_{ij} v_j$ for some $a_i, a_{ij} \in K$, and it is easy to compute that $N_1(u_i) = a_i^2 \in R$ for each i, so that $a_i \in R$. Since 1 is a basis element of P, we can subtract the a_i from each u_i and so, assume that all the u_i are in the trivial algebra. Then P is clearly a ring.

(iii) Let L be an algebra of generalized 2×2 triangular matrices with basis $1, v, u_1, \cdots, u_n$ and multiplication table as previously described. Let $1, w, t_1, \cdots, t_n$ be a basis of P over R. By the same argument used in (ii), we can assume that $w = av + \sum_{i=1}^{n} a_i u_i$, with $a, a_i \in K$. Since $N_1(1 + w) \in R$, it follows that $w + w^* \in R$, so that $a \in R$. That P is a ring now follows from the equations $w^2 = aw$, $t_i w = at_i$, $wt_i = 0$ and $t_i t_j = 0$.

This completes the proof of Theorem 2.

Bibliography

1. M. Deuring, *Algebren*, Springer, Berlin, 1935.
2. M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc., vol. 97 (1960), pp. 1–24.
3. G. R. Dirichlet and R. Dedekind, *Vorlesungen über Zahlentheorie.*
4. I. Kaplansky, *Composition of binary quadratic forms*, Studia Math.,
5. E. C. Dade, O. Taussky and H. Zassenhaus, *On the theory of orders, in particular on the semi-group of ideal classes and genera of an order in an algebraic number field*, Math. Ann., vol. 148 (1962), pp. 31–64.
6. N. Boubaki, *Algèbre Commutative*, Éléments de Mathématique, Livre XXVII, Chapter 1, §2, exercise 6, Hermann, Paris, 1965.
7. D. K. Faddeev, *An introduction to the multiplicative theory of modules of integral representations* (Russian), Trudy Mat. Inst. Steklov, vol. 80 (1965), pp. 145–182.

Roosevelt University
Chicago, Illinois